

Notice of Allowability

Application No.

10/092,277

Examiner

PONNOREAY PICH

Applicant(s)

CURRY, IAN

Art Unit

2435

– The **MAILING DATE** of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to interview held on 11/6/09, see attached interview summary.
2. ☒ The allowed claim(s) is/are 1-27.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date 11/09.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Claims 1-27 are pending. The amendments seen below are made with respect to the claims submitted on 5/12/09.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Christopher Reckamp (reg. no. 34,414) on 11/6/09. The amendments are to place the claims in condition of allowance over the prior art. The limitations added as seen in the claims have support in at least paragraph 37 of the specification. The limitations added were previously searched by the examiner (see attached applicant initiated interview summary form) thus the examiner was willing to enter the amendments after Final rejection after performing an updated search to confirm allowability of the amendments.

The application has been amended as follows:

AMEND THE FOLLOWING CLAIMS AS FOLLOWS:

1. (currently amended) A method for securing information comprising
receiving encrypted information from a sender for transmission to at least one intended recipient, receiving information indicating a transfer protocol to use when sending the encrypted information to the at least one intended recipient,

Art Unit: 2435

and receiving an encrypted secret key encrypted using a secure distribution server specific public key of a public/private key pair specific to the secure distribution server;

decrypting the encrypted secret key to produce a decrypted secret key;
obtaining a corresponding public key of the at least one intended recipient;
encrypting the decrypted secret key for the at least one intended recipient using a corresponding public key specific to the at least one intended recipient to produce at least one recipient specific secure secret key; and

forwarding, according to the information indicating the transfer protocol,
the encrypted information sent by the sender and at least one recipient specific secure key to [[for]] the at least one intended recipient.

15. (currently amended) A method for securing information comprising:

receiving, by a secure distribution server, encrypted information for transmission to a plurality of intended recipients, receiving information indicating a transfer protocol to use when sending the encrypted information to the at least one intended recipient, and receiving an encrypted secret key encrypted using a secure distribution server specific public key of a public/private key pair specific to the secure distribution server;

decrypting, by the secure distribution server, the encrypted secret key to produce a decrypted secret key;

obtaining, by the secure distribution server, a corresponding public key of at least one intended recipient;

Art Unit: 2435

encrypting, by the secure distribution server, the decrypted secret key for the at least one intended recipient using a corresponding public key specific to the at least one intended recipient to produce a recipient specific secret key; and

forwarding, by the secure distribution server, according to the information indicating the transfer protocol, the encrypted information and the recipient specific secure secret key to [[for]] a corresponding intended recipient.

18. (currently amended) A network element comprising:

one or more processing devices operative to:

decrypt a received encrypted secret key encrypted using a secure distribution server specific public key of a public/private key pair specific to the secure distribution server corresponding to the network element to produce a decrypted secret key;

obtaining a corresponding public key of at least one intended recipient;

encrypt the decrypted secret key for the at least one intended recipient using a corresponding public key specific to the at least one intended recipient to produce a recipient specific secure secret key; and

forward, to the at least one intended recipient, the encrypted information sent by a sender, according to information specified by the sender which indicates a transfer protocol to use when sending the encrypted information, and at least one recipient specific secure secret key to the at least

Art Unit: 2435

~~one intended recipient and for forwarding at least one recipient specific secure secret key for at least one corresponding intended recipient.~~

20. (currently amended) A storage medium comprising:

memory containing executable instructions that when read by one or more processing devices, causes the one or more processing devices to:

receive encrypted information from a sender for transmission to at least one intended recipient, receive information indicating a transfer protocol to use when sending the encrypted information to the at least one intended recipient, and receive an encrypted secret key encrypted using a secure distribution server specific public key of a public/private key pair specific to the secure distribution server;

decrypt the encrypted secret key to produce a decrypted secret key;

obtained a corresponding public key of the at least one intended recipient specific to the at least one intended recipient;

encrypt[[ing]] the decrypted secret key for the at least one intended recipient using the corresponding public key to produce a recipient specific secure secret key; and

forward, according to the information indicating the transfer protocol, the encrypted information sent by the sender and [[forward]] the at least one recipient specific secure key to [[for]] the at least one intended recipient.

24. (currently amended) A secure communication system comprising:

at least one sender that encrypts information with a secret key to produce encrypted information, encrypts the secret key with a secure distribution server specific public key of a public /private key pair specific to the secure distribution server associated with a network element to produce an encrypted secret key, and during an online session, sends the encrypted information and the encrypted secret key to the network element;

at least one intended recipient;

at least one network element, operatively coupled to the sender and to the at least one intended recipient, including:

one or more processing devices operative to:

decrypt a received encrypted secret key encrypted using a secure distribution server specific public key of a public/private key pair specific to the secure distribution server corresponding to the network element to produce a decrypted secret key;

obtaining a corresponding public key of at least one intended recipient;

encrypt the decrypted secret key for the at least one intended recipient using a corresponding public key specific to the at least one intended recipient to produce a recipient specific secure secret key; and

forward, to the at least one intended recipient, the encrypted information sent by a sender, according to information specified by the sender

Art Unit: 2435

which indicates a transfer protocol to use when sending the encrypted information and at least one recipient specific secure secret key to the at least one intended recipient and forwarding at least one recipient specific secure secret key for at least one corresponding intended recipient.

The following is an examiner's statement of reasons for allowance: The prior art does not teach the combination of limitations as currently recited in any of above claims 1, 15, 18, 20, and 24. Perlman, used in the last Office action to reject the claims, is the closest prior art. However, Perlman does not teach that the a receiver also receives (i.e. from a sender) information specified by the sender which indicates a transfer protocol to use when sending/forwarding the encrypted information (i.e. encrypted message) and at least one recipient specific secure secret key to the recipient and then forwarding according to the specified transfer protocol. Support for this limitation can be found in at least paragraph 37 of the specification. Using claim 1 as an example claim, read in light of the specification, what this limitation essentially means is that the sender "programs" the entity that carries out the method of claim 1 (i.e. the SDS as discussed in the specification) to use a specific information transport protocol when forwarding the encrypted message and encrypted message key. Typically, when an intermediary (i.e. SDS as discussed in the specification) receives a particular type of message, it merely forwards the message using whatever type of protocol that was used to send the message initially. However, in the case of the above

Art Unit: 2435

independent claims, the sender is controlling the particular protocol used (i.e. by the SDS as discussed in the specification) to forward to the recipient(s). The remaining claims are allowed due to dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2435

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Primary Examiner, Art Unit 2435